

# North Carolina Statewide Technical Architecture

---

Network Domain

©2005 State of North Carolina  
Office of the State Chief Information Officer  
Enterprise Technology Strategies  
PO Box 17209  
Raleigh, North Carolina 27699-7209  
<http://www.ncsta.gov>  
[ets@ncmail.net](mailto:ets@ncmail.net)

All rights reserved. No part of the material protected by this copyright notice may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording or by any informational storage system without written permission from the copyright owner.

## Table of Contents

<b>1. PRINCIPLES .....</b>	<b>4</b>
1.1. NETWORKS ARE ABLE TO ADAPT TO GROWTH AND TECHNOLOGY CHANGE WHEN THEY SUPPORT MULTIPLE TRAFFIC TYPES (E.G. DATA, VIDEO, VOICE).....	4
1.2. NETWORK ACCESS IS A FUNCTION OF AUTHENTICATION AND AUTHORIZATION, NOT OF LOCATION. 4	
1.3. FULLY AVAILABLE NETWORKS ARE ESSENTIAL TO THE ENTERPRISE. ....	4
1.4. PROPERLY DESIGNED NETWORKS ACCOMMODATE MULTI-VENDOR PARTICIPATION AND SUPPORT COMMON, OPEN, VENDOR-NEUTRAL PROTOCOLS. ....	5
<b>2. LOCAL AREA NETWORK.....</b>	<b>5</b>
2.1. PRACTICES .....	5
2.1.1. <i>Maintain detailed diagrams and documentation for all local area networks.</i> .....	5
2.1.2. <i>Include network performance monitoring as part of the overall performance management strategy.</i> 6	
2.1.3. <i>Disable all unused ports on network devices.</i> .....	6
2.2. STANDARDS .....	6
2.2.1. <i>The standard for LAN cabling is Category 5, 5e, or 6Unshielded Twisted Pair (Cat 5 UTP, Cat 5e UTP, or Cat 6 UTP). ....</i>	6
2.2.2. <i>The standard for standard link layer access protocol is Ethernet, IEEE 802.3 Carrier Sense Multiple Access/Collision Detection Access Method (CSMA/CD). ....</i>	6
<b>3. WIDE AREA NETWORK.....</b>	<b>7</b>
3.1. PRACTICES .....	7
3.1.1. <i>Utilize the centrally maintained and managed enterprise-wide network infrastructure. ....</i>	7
3.1.2. <i>Size WAN links based on documented analysis of aggregate bandwidth requirements.</i> .....	7
3.2. STANDARDS .....	7
3.2.1. <i>The standard protocol technology is TCP/IP. ....</i>	7
3.2.2. <i>The standard internet access technology is Domain Name System (DNS) and IP address assignments are provided by State Information Technology Services (ITS) for those agencies participating in the North Carolina Integrated Information Network (NCIIN). ....</i>	7
<b>4. NETWORK-CENTRIC APPLICATIONS.....</b>	<b>8</b>
4.1. PRACTICES .....	8
4.1.1. <i>Include network expertise on the requirements and system design teams. ....</i>	8
4.1.2. <i>Design network-neutral applications.</i> .....	8
4.1.3. <i>Plan data movement. ....</i>	8
4.1.4. <i>Consider the impact of middleware on network utilization. ....</i>	9
4.1.5. <i>Deploy heavily used data sources "close" to the applications using them. ....</i>	9
4.1.6. <i>Limit dependency on the network by designing applications with coarse-grained interfaces.</i> 9	
4.1.7. <i>Perform performance measurement and load testing on distributed applications before deployment.</i> .....	9
<b>5. WIRELESS COMMUNICATIONS.....</b>	<b>10</b>
5.1. PRACTICES .....	10
5.1.1. <i>Implement a layered approach to wireless security.</i> .....	10
5.1.2. <i>Develop a shared key distribution process prior to implementation. ....</i>	10
5.1.3. <i>SNMP must be disabled on wireless networking and communications devices unless explicitly required.</i> .....	11
5.1.4. <i>Wireless management and configuration tools must not be used over the wireless medium.</i> 11	
5.1.5. <i>Use the Extended Service Set Identifier (ESSID) for network partitioning and not as a security control. ....</i>	11
5.1.6. <i>Periodically analyze the network to discover unauthorized devices.</i> .....	12
5.1.7. <i>For secure data transfer using infrared, implement application, network, and physical access security measures. ....</i>	12

5.1.8.	<i>Determine access point placement based on a documented site survey.</i>	12
5.2.	STANDARDS	12
5.2.1.	<i>Implement only WECA Wi-Fi™ certified devices in a wireless network to ensure interoperability.</i>	12
5.2.2.	<i>Use IrDA® certified devices when using infrared communication.</i>	13
5.2.3.	<i>Use only WLAN devices that comply with IEEE 802.11.</i>	13
5.2.4.	<i>Use only WMAN devices that comply with IEEE 802.16.</i>	13

# 1. Principles

## 1.1. Networks are able to adapt to growth and technology change when they support multiple traffic types (e.g. data, video, voice).

Rationale:

- The increasing investment of funds in network infrastructures dictates that the life span of each additional component or enhancement be as long as possible. This can be accomplished if the design supports both current needs and anticipated growth potential.
- As businesses expand, networks expand. A flexible, open network design will allow a business to minimize the costs and disruptions of configuration management while providing timely and responsive network changes when and where required.

## 1.2. Network access is a function of authentication and authorization, not of location.

Rationale:

- All users must obtain authentication via a user identification method consistent with the standards and usage guidelines set by the enterprise.
- Authorization of users must be performed according to the security rules of the enterprise and the local business unit.
- In order to perform their job functions, users need to access services available from multiple sites within the enterprise, from a variety of public and private networks, and from the Internet.

## 1.3. Fully available networks are essential to the enterprise.

Rationale:

- Networks provide an increasingly important and necessary role in the execution of business functions and processes. The availability of the network seven days a week and twenty-four hours a day must be maintained in a consistent and complete manner.
- Networks consist of and rely on many interrelated and often highly complex components distributed across a wide geographic area. Failure of any single component can have severe adverse effects on one or more business applications or services.
- Reliable networks contain no single point of failure. Networks are comprised of many components, and are often only as reliable as the weakest link. Therefore, reliability and redundancy must be built into the design, not added-on in an ad hoc manner.
- Bandwidth must be sufficient to accommodate new and expanding applications, different types of data (e.g., voice, data, image, and video), and a variety of concurrent users.
- The network must support software distribution and installation to a widely dispersed user community.
- The network must be designed to minimize latency.

## **1.4. Properly designed networks accommodate multi-vendor participation and support common, open, vendor-neutral protocols.**

Rationale:

- Open, vendor-neutral protocols provide the flexibility and consistency that allows agencies to respond more quickly to changing business requirements.
- Open, vendor neutral networks provide the flexibility and consistency that allows agencies to respond more quickly to changing business requirements.
- An open, vendor-neutral network allows the state to choose from a variety of sources and select the most economical network solution without impacting applications.
- This approach supports economic and implementation flexibility because technology components can be purchased from many vendors. This insulates the state from unexpected changes in vendor strategies and capabilities.
- Design applications to be transport-independent.

## **2. Local Area Network**

### **2.1. Practices**

#### **2.1.1. Maintain detailed diagrams and documentation for all local area networks.**

Rationale:

- Network documentation is a critical tool to help maintain control over network security, aid in troubleshooting, and maintain continuity and availability. Structure network documentation such that any competent network engineer could use the documentation to effectively manage and troubleshoot the network. Typical network documentation includes, but is not limited to:
- Diagrams of the network topology including placement of servers, routers, switches, firewalls, IDS, etc.
- Network Operations Procedures
  - IP Subnet allocations
  - VLAN setup
  - Maintenance contracts
  - Emergency contacts
  - Vulnerability Scan Procedures
  - Disaster Recovery Procedures
- Network Configuration
  - Documentation of all devices such as routers, switches, access points, firewalls, end device NICs (e.g. PCs, servers, printers) with IP addresses, port number, domain name with expiration, NetBOIS/Server Name, Location, Brand/Model/Serial Number, Line Speed, MAC Address, Community Strings/Passwords, Owner, etc.
  - Retain all receipts from products purchased.
  - DHCP server settings including scope and options.
  - Firewall configuration

- Router access lists
- Troubleshooting history and administrator activity log.

### **2.1.2. Include network performance monitoring as part of the overall performance management strategy.**

Rationale:

- Network performance monitoring is a key factor in determining the performance characteristics of an implemented system.
- Baseline networks initially to establish a reference point to be used in contrast to continuing performance monitoring.
- Network baseline information can include:
  - Traffic flow and network utilization.
  - Bandwidth utilization.
  - Percent of collisions.

### **2.1.3. Disable all unused ports on network devices.**

Rationale:

- Allocation of a port on a network device must be planned and tied to a known end device.
- Disable all ports that are not directly assigned to a known end device in order to reduce the chances of port misuse.
- Do not attach unused network device ports to patch panels or other inactive or unused network devices.

## **2.2. Standards**

### **2.2.1. The standard for LAN cabling is Category 5, 5e, or 6Unshielded Twisted Pair (Cat 5 UTP, Cat 5e UTP, or Cat 6 UTP).**

Rationale:

- Unless specific needs exist, such as high EMI or long distances, use UTP for the horizontal runs in cable layouts. Vertical runs may utilize UTP or optical fiber.
- CAT 5/5e/6UTP can be certified to carry 10/100/1000 MBPS of data.
- It is an industry standard wiring plan and has the support of the IEEE.
- Wiring, cable, connector, and equipment vendors have standardized on this cabling.

### **2.2.2. The standard for standard link layer access protocol is Ethernet, IEEE 802.3 Carrier Sense Multiple Access/Collision Detection Access Method (CSMA/CD).**

Rationale:

- Widely accepted format.
- Reliable, the protocol has been used for years and is very stable.

## **3. Wide Area Network**

### **3.1. Practices**

#### **3.1.1. Utilize the centrally maintained and managed enterprise-wide network infrastructure.**

Rationale:

- A single uniform network infrastructure allows an enterprise to respond more efficiently when faced with requests by agencies for WAN component upgrades and installation.
- A centrally developed and managed infrastructure provides a more cost effective use of infrastructure resources.
- Focus WAN requirements on functional specifications such as level of service needed, throughput needed, and response time needed. The implementation of an appropriately responsive WAN is a specialized function performed for the enterprise in its entirety.

#### **3.1.2. Size WAN links based on documented analysis of aggregate bandwidth requirements.**

Rationale:

- Reduces risk of performance problems with mission critical systems.
- Provides an understanding of usage profiles and enables agencies to begin prioritization of traffic by eliminating high-bandwidth consuming applications like streaming video.
- Right sizing WAN links ensures the best value proposition.

### **3.2. Standards**

#### **3.2.1. The standard protocol technology is TCP/IP.**

Rationale:

- Open protocol.
- Allows Internet access.
- Allows creation of Intranets and VPNs.

#### **3.2.2. The standard internet access technology is Domain Name System (DNS) and IP address assignments are provided by State Information Technology Services (ITS) for those agencies participating in the North Carolina Integrated Information Network (NCIIN).**

Rationale:

- ITS must assign IP addresses to allow LANs access to the NCIIN State WAN.
- All Internet access is provided by the NCIIN and is controlled by the state's Domain Name System.

- It allows a structured naming convention and IP address allocation for the state's WAN and domain names.

## **4. Network-Centric Applications**

### **4.1. Practices**

#### **4.1.1. Include network expertise on the requirements and system design teams.**

Rationale:

- Including network expertise ensures correct planning, documentation, and standard practices are followed.
- Include application performance requirements definition, as well as capacity planning for network usage (based on the predicted number and size of transactions).
- Define any special networking requirements or constraints and perform the associated network design before development tools are selected. Otherwise, the tools used may not support the network architecture required to support the business.
- The network can be modified (upgraded) as appropriate while applications are under development.
- Balance performance and the cost to move information during application design. Multiple perspectives of a cross-functional group can ensure all viable options are considered.

#### **4.1.2. Design network-neutral applications.**

Rationale:

- Isolate the application code from the network specific code so business rules and data access code can be reconfigured and not reliant on underlying platform or network configuration.
- For a network to remain scalable and portable, applications must be developed without regard to the type of network (i.e. WAN or LAN) they are to be deployed on.
- Network-specific design (e.g., wireless or guaranteed high-bandwidth) should only be performed when business requirements dictate.

#### **4.1.3. Plan data movement.**

Rationale:

- When possible, schedule heavy network use for off-peak hours. For example, where requirements for data freshness permit, perform database synchronization at night.
- Data warehouses typically are used for decision support applications requiring large amounts of data to be transferred through the network.
- When replicating databases, consider partitioning and distributing subsets, rather than duplicating the entire master database.
- Decoupling the application layers provides the most efficient use of network resources by allowing the data access layer to be placed near the data.

**4.1.4. Consider the impact of middleware on network utilization.**

Rationale:

- Perform all transaction commits locally, between the resource manager and the queue. Asynchronous store and forward messaging can limit the scope of a transaction.
- Decouple transactions as allowed by business rules.
- Reconcile data at low-cost times.
- Using store and forward, work can occur at a site even if the network link is down.

**4.1.5. Deploy heavily used data sources "close" to the applications using them.**

Rationale:

- "Close" does not imply physical proximity. It means deployed on platforms that have high-bandwidth connections between them. Do not perform heavy data movement across the WAN during peak hours.
- One of the biggest cost factors in designing a network is the transmission of the data over the communications system.
- For applications requiring very large amounts of data movement, try scheduling the execution of queries to run during off peak hours to minimize the impact on network performance.

**4.1.6. Limit dependency on the network by designing applications with coarse-grained interfaces.**

Rationale:

- Minimize the amount of data to be moved between components. This will enhance performance regardless of the speed of the network on which the application is deployed.
- Use asynchronous rather than synchronous communications between application components (except in cases where business rules require synchronous communications). This will prevent application components waiting for a response from a server.
- For users and application requests that may be intermittently connected, use store-and-forward messaging to communicate with application components.
- When multiple, independent units of work must be performed, initiate all so they can be performed in parallel, rather than waiting for the completion of one before initiating the next.

**4.1.7. Perform performance measurement and load testing on distributed applications before deployment.**

Rationale:

- Measure application performance often, especially before and after any component is moved to a different platform. This helps quantify the performance impact of the redeployment, and helps isolate any problems associated with a network link or platform.

- Use load-testing tools that simulate many users accessing the application. This testing method will provide information that will not surface during single user test scenarios.
- Load testing will identify network bottlenecks (and application bottlenecks) before the application is deployed in the production environment.

## **5. Wireless Communications**

### **5.1. Practices**

#### **5.1.1. Implement a layered approach to wireless security.**

Rationale:

- No single security approach is sufficient to secure wireless communications. For example, VPNs add an important layer of protection by encrypting the data flow. However, VPNs are not sufficient on their own; they must be used within an environment of strong authentication in concert to achieve a comprehensive security solution.
  - Change the default Enterprise Service Set Identifier (ESSID) on wireless access points.
  - Filter based on Media Access Control (MAC) address of the client.
  - Disable access to wireless access points via "wildcard" ESSID's.
  - Enable 128-bit Wired Equivalent Privacy (WEP) to encrypt data transmission using Fast Packet Keying (FPK).
  - Place wireless access points outside the firewall in the DMZ.
  - Require user authentication and authorization in order to gain access to the wireless network.
  - Utilize Virtual Private Networking (VPN) where strong security is required.
  - Provide application level security such as application authentication and authorization as well as SSL.
- Not all security measures in the list above are required. Some negate the need for others e.g. if implementing VPN, WEP may cause unnecessary overhead while providing little additional security benefit. Some may disable a desired feature e.g. "wildcard" (enabling clients to automatically detect the access point) ESSID's can be an effective tool for granting guest access to a wireless access point in order to access the Internet.
- It is important to note that; in order to secure a wireless network there isn't a single solution, many security measures must be layered to ensure the integrity of the data., network controls, and sound security policies and practices. Therefore, several security practices should be employed.

#### **5.1.2. Develop a shared key distribution process prior to implementation.**

Rationale:

- The Wired Equivalent Privacy (WEP) standard uses a shared key system. The WEP standard does not, however, include a process for distributing pass-phrases, hex keys, or ASCII strings that represent a wireless encryption key. Therefore, a secure process

for the distribution and maintenance of shared keys must be developed in advance of implementation in order to ensure the security of the data.

- NOTE: WEP only encrypts the transmission between the workstation and the access point or another radio NIC. Once the traffic enters the wired network, WEP no longer applies and where encryption is required on the wired network, other technologies must be employed.

### **5.1.3. SNMP must be disabled on wireless networking and communications devices unless explicitly required.**

Rationale:

- Networking and communications devices often include the ability to monitor and manage the device using SNMP. However, manufacturers that have SNMP functionality, set a default community string (i.e. a password) that is common among all devices of that model or brand. Therefore, a significant security exposure exists unless the community string is changed or SNMP is disabled.
- SNMP vulnerabilities may cause denial-of-service conditions, service interruptions, and in some cases may allow an attacker to gain access to the affected device. Specific impacts will vary from product to product.
- Due to these exposures, SNMP must be disabled unless explicitly required. If there is a requirement for SNMP, the default community string must be changed on a regular basis and SNMP must not traverse the wireless medium.
- NOTE: Changing the community string does NOT overcome the vulnerabilities that exist in SNMP; it only addresses one specific exposure.
- The CERT® Coordination Center also recommends disabling SNMP on all devices (including wireless) unless it is explicitly required.

### **5.1.4. Wireless management and configuration tools must not be used over the wireless medium.**

Rationale:

- Management and configuration tools have defined rights to control network devices and have greater access rights than the typical client. Since wireless networks have no physical boundaries to protect the environment, as does its wired counterpart, it may be possible to capture information about a management or configuration tool and obtain access posing as the device.
- Therefore, management and configuration of wireless devices must be performed over the wired medium and local to the device that is being controlled.
- The level of access that is commonly apportioned to management and configuration tools must be disabled from the wireless network over the wireless medium.

### **5.1.5. Use the Extended Service Set Identifier (ESSID) for network partitioning and not as a security control.**

Rationale:

- A wireless device attempting to connect to a wireless network must provide the ESSID of the wireless access point device before it is permitted to join. The ESSID is the same for all users connecting to the access point and is transmitted in plain text.

Often, using the ESSID "ANY" (also known as a "wildcard" ESSID) enables the device to automatically detect the ESSID of the wireless access point with the strongest signal and connect.

- The ESSID should not be considered private or secure. However, the ESSID provides an effective means of partitioning wireless networks in that connection is established only with the intended access point not based on signal strength.

#### **5.1.6. Periodically analyze the network to discover unauthorized devices.**

Rationale:

- Wireless access points can be deployed without the knowledge of the organization. If implemented incorrectly, rogue devices may create serious security exposures.
- A periodic analysis of the network will uncover these rogue devices. At that time, the device may be assessed for compliance with the standard practices and standards and either removed from the network or formally established within the network as a compliant device.
- Perform this analysis at least annually.

#### **5.1.7. For secure data transfer using infrared, implement application, network, and physical access security measures.**

Rationale:

- The Infrared Data Association (IrDA®) standards do not specify security for data transfer.
- Since line-of-sight is required and distance limitations (Less than 1 meter) exist for data transfer, a minimal level of security is achieved based on proximity.
- Security of the data transfer is dependent upon physical access to the infrared devices and application and/or network access controls.
- Therefore, if security is required for data transfer using IrDA® standards, application, network, and physical security measures must be implemented

#### **5.1.8. Determine access point placement based on a documented site survey.**

Rationale:

- Wireless installations differ at each facility. These unique properties must be addressed in order to ensure that the coverage requirement at your location is complete.
- There are various techniques in performing a site survey including the use of automated tools.
- Regardless of the mechanism selected, a site survey must be documented and kept up-to-date.

## **5.2. Standards**

### **5.2.1. Implement only WECA Wi-Fi™ certified devices in a wireless network to ensure interoperability.**

Rationale:

- The Wireless Ethernet Compatibility Alliance (WECA) mission is to certify interoperability of Wireless Fidelity (Wi-Fi™), IEEE 802.11b High Rate Standard, products and to promote Wi-Fi™ as the global wireless LAN standard across all market segments.
- Most major manufacturers of wireless devices have willingly undergone the certification process and successfully complied with the standards.

### **5.2.2. Use IrDA® certified devices when using infrared communication.**

Rationale:

- The Infrared Data Association (IrDA®) is an international non-profit standards organization that certifies products, which pass the standard IrDA® Interoperability Tests conducted by independent test labs. Products certified typically display the IrReady® Logo.
- Use of this standard will ensure interoperability among devices implemented from varying vendors.

### **5.2.3. Use only WLAN devices that comply with IEEE 802.11.**

Rationale:

- The Institute of Electrical and Electronics Engineers, Inc. (IEEE) is a non-profit, technical professional association of more than 375,000 individual members in 150 countries. The State of North Carolina Office of Information Technology Services maintains membership with the IEEE.
- Through its members, the IEEE is a leading authority and standards body in technical areas ranging from computer engineering, biomedical technology and telecommunications, to electric power, aerospace, and consumer electronics, among others. The IEEE also established standards for Ethernet 802.3.
- Extending the standard wired LAN environment to wireless should also utilize the concepts and approach of Ethernet. This helps to ensure interoperability among wired and wireless LAN environments.

### **5.2.4. Use only WMAN devices that comply with IEEE 802.16.**

Rationale:

- The IEEE 802.16 standard provides the framework by which most wireless fixed point to multi-point broadband devices are developed.
- Adoption of this standard also provides the highest degree of interoperability with wired and wireless LANs.